WHAT IS CLAIMED:

1. A method of enforcing security policies in a data access system, said method comprising:

defining a first action as a condition;

determining that a second action should not take place if said condition occurs;

storing a rule for use by said data access system, said rule precluding said second action; and

upon occurrence of said condition, utilizing said rule in said data access system.

2. The method of claim 1 wherein said condition is effectuation of a first transaction by a user and said second action is the effectuation of a related transaction by the same user.

3. The method of claim 1 wherein said condition is effectuation of a first transaction by a first user in a particular role, and said second action is the effectuation of a second transaction by a second user in a second role, the roles being either the same or different.

4. The method of claim 3 wherein the role of the first user and that of the second user are different.

5. The method of claim 2 wherein the condition is effective temporarily and than is rescinded.

6. The method of claim 2 wherein a user attempting to effectuate said related transaction is informed of said condition and advised automatically that said second action is prohibited pending the relinquishment of the condition.

7. The method of claim 2 wherein said first action is the ordering of goods or services and said second action is the payment for such goods or services.

8. Apparatus for enforcing security policies to increase security of data access management software, said apparatus comprising:

a file of rules, said rules only being applicable to prevent specified data transactions by a first user upon the effectuation of specified transactions to modify the data by said first user;

software for recognizing that said first user has effected said transaction, and

means for reading said file, locating said rules to prevent said specified data transactions, and integrating said rules into said data access management software such that said specified database transactions are prohibited.

9. Apparatus of claim 8 wherein further comprising means for eliminating the rule from the data access management software at the conclusion of a predetermined time or upon a predetermined condition.

10. A method of enforcing confidentiality in the form of a wall comprising the steps of:

storing at least one rule that prohibits a known party from accessing specified information in a database or file;

upon a first specified condition occurring, modifying data access software to include said rule that prohibits said known party from accessing said specified information in a database or file;

said first specified condition being indicative of said known party having knowledge of a particular set of information; and

upon a second specified condition occurring, removing said rule and storing said rule for future use, said specified second condition indicating that said knowledge is no longer sensitive.

11. The method of claim 10 wherein said rule is generated from a template rule.

12. The method of claim 11 wherein said known party is defined as any individual engaged in a predetermined role.

13. The method of claim 10 wherein said user is notified of the occurrence of said second condition.

14. The method of claim 13 wherein said notification is via email.

15. The method of claim 10 wherein said knowledge is no longer sensitive because it has been made public or because a predetermined time has passed.

16. The method of claim 1 wherein said rule is generated from a template rule.

17. The method of claim 10 wherein some other individual, not the user, is notified of the occurrence of said second condition.

18. The method of claim 16 wherein said notification is via e-mail.

19. The method of claim 2 wherein some other individual, not the user, is notified of the occurrence of said second condition.

20. The method of claim 18 wherein said notification is via e-mail.

21. The method of claim 6 wherein the notification is via e-mail.

22. The method of claim 2 wherein another individual, not the user, is notified when the user attempts the prohibited second action more than once.

23. The method of claim 10 wherein another individual, not the user, is notified when the user attempts the prohibited second action more than once.

24. The method of claim 21 wherein the notification is via e-mail.

25. The method of claim 22 wherein the notification is via e-mail.

26. The method of claim 21 wherein the other individual is the users manager or supervisor.

27. The method of claim 21 wherein the other individual is responsible for data security.

28. The method of claim 22 wherein the other individual is the users manager or supervisor.

29. The method of claim 22 wherein the other individual is responsible for data security.

30. The method of claim 9 wherein the eliminated rule is saved in an audit log.

31. The method of claim 10 wherein the eliminated rule is saved in an audit log.

32. The method of claim 1 wherein the rule is not loaded until the specified user logs on to the system.

33. The method of claim 1 wherein the rule is only tested for the specified user.

34. The method of claim 10 wherein the rule is not loaded until the specified user logs on to the system.

35. The method of claim 10 wherein the rule is only tested for the specified user.

36. The method of claim 3 wherein the rule is not loaded until a user in the specified role logs on to the system.

37. The method of claim 3 wherein the rule is only tested for a user in the specified role.

38. The method of claim 12 wherein the rule is not loaded until a user in the specified role logs on to the system.

39. The method of claim 12 wherein the rule is only tested for a user in the specified role.

40. The method of claim 1 wherein the security policy is separation of duties.

41. The method of claim 1 wherein the security policy is compliance to regulation.

42. The method of claim 1 wherein the security policy is privacy of data.

43. The method of claim 21 wherein the other individual is a computer process.

44. The method of claim 22 wherein the other individual is a computer process.